DETAILED ACTION

1. In response to amendment filed on 24 March 2008 and Examiner Initiated Interview on 16 April 2008. Claims 1, 17, 23, and 25-27 are amended. Claims 3, 18, 28-42, 51, and 53 are canceled.

2. An examiner's amendment to the record is attached. Please enter entire claim set. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. The examiner's amendment was authorized by attorney of record Victor G. Cooper in a phone interview on 16 April 2008.

3. The IDS submitted 25 March 2008 has been considered.

Response to Arguments

4. Applicant's arguments filed 24 March 2008 have been fully considered and they are persuasive.

Allowable Subject Matter

5. Claims 1, 2, 4-17, 19-27, 43-50, and 52 are allowed.

Conclusion

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/ELLEN TRAN/
Primary Examiner, Art Unit 2134
18 April 2008

Examiner's Amendment

This listing of the claims will replace all prior versions and listings of the claims in the application:

Listing of Claims:

1. (CURRENTLY AMENDED) A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising the steps of:

(a) accepting a data stream including data packets with ~~encrypted access control information and the~~ program material encrypted according to a first encryption key and access control information which is contained within one or more control word packets that include an encrypted version of the first encryption key in the receiver ~~, the access control information including a first encryption key and control data~~;

(b) decrypting the received access control information in a conditional access module ~~releasably coupleable~~ which is releasably communicatively coupled with the receiver to produce the first encryption key;

(c) decrypting the program material in the receiver using the first encryption key;

(d) re-encrypting the program material according to a second encryption key;

(e) encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key; and

(f) providing the re-encrypted program material and the fourth encryption key for storage external to the conditional access module.

2. (CURRENTLY AMENDED) The method of claim 1, wherein the encrypted access control information is encrypted and further comprises temporally-variant control data, and the method further comprises the steps of:

decrypting the received access control information to produce the temporally-variant control data; and

modifying the temporally variant control data to generate temporally-invariant control data.

3. (CANCELED)

4. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the conditional access module is implemented on a smartcard.

5. (ORIGINAL) The method of claim 1, wherein the access control information further comprises metadata describing at least one right for the program material.

6. (ORIGINAL) The method of claim 5, further comprising the step of:

generating the second encryption key at least in part from the metadata.

7. (ORIGINAL) The method of claim 1, wherein steps (b)-(f) are performed in response to a pre-buy message.

8. (ORIGINAL) The method of claim 7, wherein the access control information further comprises metadata describing at least one right for the program material, and the method further comprises the step of:

generating replay right data from the metadata.

9. (ORIGINAL) The method of claim 8, wherein the replay right data is further generated from pre-buy data.

10. (ORIGINAL) The method of claim 1, further comprising the steps of:

retrieving the stored re-encrypted program material and the fourth encryption key;

decrypting the fourth encryption key using the third encryption key to produce the second encryption key; and

decrypting the re-encrypted material using the second encryption key.

11. (ORIGINAL) The method of claim 10, wherein the step of decrypting the fourth encryption key using the third encryption key to produce the second encryption key is performed in response to a subscriber request to access the program material.

12. (ORIGINAL) The method of claim 11, wherein the access control information further comprises metadata describing at least one right for the program material, the subscriber request to access the program material comprises buy data, and the method further comprises the steps of:

generating replay right data from the metadata;

accepting the buy data;

comparing the buy data with the replay right data; and

decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data.

13. (ORIGINAL) The method of claim 12, wherein steps (b)-(f) are performed in response to a pre-buy message, and wherein:

the second encryption key and the third encryption key are stored in a smartcard, and the replay right data is generated from the metadata and the pre-buy message in the smartcard; and

the steps of accepting the buy data, comparing the buy data with the replay right data, and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data are performed in the smartcard.

14. (ORIGINAL) The method of claim 1, wherein the re-encrypted program material and the fourth encryption key are stored on a media storage device.

15. (ORIGINAL) The method of claim 1, wherein the control data is temporally-variant.

16. (ORIGINAL) The method of claim 15, wherein the temporally-variant control data associates an expiration time with the program material.

17. (CURRENTLY AMENDED) An apparatus for storing program material encrypted according to a first encryption key for replay, comprising:

a conditional access module, for accepting encrypted access control information including the first encryption key and temporally-variant control data, the control access module comprising:

a first decryption module, for decrypting the access control information to produce the first encryption key;

a ~~first~~ second encryption module, for encrypting a second encryption key with a third encryption key to produce a fourth encryption key for storage external to the conditional access module; and

a ~~second~~ third decryption module for decrypting the fourth encryption key to produce the second encryption key;

wherein the conditional access module is releasably communicatively coupled to a tuner, the tuner to enable reception of the encrypted access control information and the program material encrypted according to a first encryption key, the tuner comprising:

a ~~third~~ second decryption module, for decrypting the program material using the first encryption key produced by the conditional access module;

a ~~second~~ first encryption module, for re-encrypting the decrypted program material according to the second encryption key; and

a fourth decryption module, for decrypting the re-encrypted program material according to the second encryption key.

18. (CANCELED)

19. (PREVIOUSLY PRESENTED) The apparatus of claim 17, wherein the conditional access module further comprises:

a pre-buy module, for controlling the first decryption module.

20. (PREVIOUSLY PRESENTED) The apparatus of claim 17, wherein the access control information further comprises metadata describing at least one right for the program material.

21. (PREVIOUSLY PRESENTED) The apparatus of claim 20, wherein:

the conditional access module comprises a pre-buy module for controlling the first decryption module, and for generating replay right data from the metadata.

22. (ORIGINAL) The apparatus of claim 21, further comprising a buy module, communicatively coupled to the pre-buy module.

23. (CURRENTLY AMENDED) The apparatus of claim 22, wherein the buy module comprises:

a purchase module for accepting buy data and comparing the buy data and the replay right data from the pre-buy module; and

a control module for controlling the ~~second~~ third decryption module based on the comparison between the buy data and the replay right data.

24. (ORIGINAL) The apparatus of claim 23, further comprising a billing module, for recording the buy data.

25. (CURRENTLY AMENDED) The apparatus of claim [[18]] 17, wherein the second encryption key is stored in the conditional access module.

26. (CURRENTLY AMENDED) The apparatus of claim [[18]] 17, wherein the third encryption key is stored in the conditional access module.

27. (CURRENTLY AMENDED) The apparatus of claim 17, wherein the conditional access module is releaseably communicatively ~~couplable~~ coupled to:

a tuner for receiving the encrypted access control information and the program material encrypted according to a first encryption key;

a ~~third~~ second decryption module, for decrypting the program material using the first encryption key from the conditional access module

a ~~second~~ first encryption module, for re-encrypting the decrypted program material according to the key; and

a media storage device.

28. - 42. (CANCELED)

43. (PREVIOUSLY PRESENTED) The method of claim 1, further comprising the step of generating the second encryption key in the conditional access module.

44. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the access control information further comprises metadata and the method further comprises the step of generating the second encryption key at least in part from the metadata.

45. (PREVIOUSLY PRESENTED) The method of claim 1, further comprising the step of:

augmenting the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module.

46. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the access control information further comprises metadata describing at least one right for the program material, and the method further comprises the step of:

augmenting the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module.

47. (PREVIOUSLY PRESENTED) The apparatus of claim 20, wherein the conditional access module generates the second encryption key at least in part from the metadata.

48. (PREVIOUSLY PRESENTED) The apparatus of claim 17, wherein the access control information further comprises metadata and the conditional access module generates the second encryption key at least in part from the metadata.

49. (PREVIOUSLY PRESENTED) The apparatus of claim 20, wherein the conditional access module augments the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module.

50. (PREVIOUSLY PRESENTED) The apparatus of claim 17, wherein the access control information further comprises metadata, and wherein the conditional access module augments the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module.

51. (CANCELED)

52. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the second encryption key is stored in the conditional access module.

53. (CANCELED)

/ELLEN TRAN/

Primary Examiner, Art Unit 2134